



专题：智能边缘计算

基于边缘计算的铁路施工项目安全监管数据共享研究

杨亮¹, 朴春慧^{1,2}, 刘玉红^{1,2}, 冀梅梅¹

(1. 石家庄铁道大学信息科学与技术学院, 河北 石家庄 050043;

2. 河北省电磁环境效应与信息处理重点实验室, 河北 石家庄 050043)

摘 要: 信息化安全监测系统在铁路施工项目中应用广泛, 但现有的安全监管模式存在服务器负载高、网络带宽压力大、监测数据不能有效共享、关键监测数据可能被篡改、安全事故责任难以确定等问题。提出了基于边缘计算的铁路施工项目安全监管数据可信共享模式: 一方面, 构建了施工项目安全监测边缘计算框架, 描述了边缘节点数据处理流程; 另一方面, 建立了基于区块链的数据可信共享框架, 设计了安全监管数据共享流程, 通过智能合约实现数据可信共享。本文提出的解决方案融合运用边缘计算技术和区块链技术, 不仅能够加强行业主管部门对于铁路施工项目的安全监管, 还为利益相关方实时共享安全监测数据、提高施工项目安全管理水平提供了新的思路。

关键词: 铁路施工项目; 安全监管; 边缘计算; 区块链; 可信共享

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2020172

Research on safety supervision data sharing of railway construction projects based on edge computing

YANG Liang¹, PIAO Chunhui^{1,2}, LIU Yuhong^{1,2}, JI Meimei¹

1. School of Information Science and Technology, Shijiazhuang Tiedao University, Shijiazhuang 050043, China

2. Hebei Key Laboratory for Electromagnetic Environmental Effects and Information Processing, Shijiazhuang 050043, China

Abstract: Information security monitoring system is widely used in railway construction projects, but the existing safety supervision model has problems such as high server load, heavy network bandwidth pressure, monitoring data can't be effectively shared, key monitoring data may be tampered, and security accident responsibility is difficult to determine. A credible sharing model of safety supervision data for railway construction projects based on edge computing was proposed. On one hand, the construction of a safety monitoring edge computing framework for construction projects was constructed, and the data processing flow of edge nodes was described; on the other hand, a trusted data sharing framework based on blockchain was established, and a safety supervision data sharing process was designed and trusted sharing data was implemented through smart contracts. The proposed solution combined with edge computing and blockchain technology, which not only could strengthen the safety supervision of railway construction projects by industry authorities, but also provide new opportunities for stakeholders to share safety monitoring data in real time.

Key words: railway construction project, safety supervision, edge computing, blockchain, trusted sharing

收稿日期: 2020-04-01; 修回日期: 2020-05-28

通信作者: 刘玉红, lyhlkw@sina.com

基金项目: 河北省研究生创新资助项目 (No.CXZZSS2020073)

Foundation Item: Graduate Innovation Foundation of Hebei Province (No.CXZZSS2020073)

1 引言

交通强国铁路先行,习近平总书记在党的十九大报告中提出建设社会主义现代化强国,并将交通强国作为其中的重要内容,纳入国家未来几十年的发展战略之中^[1]。交通强国战略的提出,促进了我国交通运输行业的发展,以高速铁路建设为主的铁路工程项目也逐年增加。由于铁路项目建设范围广、里程长,因此采取有效的手段监测铁路施工项目过程中的异常点和异常程度,对铁路施工项目的施工安全有十分重要的意义^[2]。

中国国家铁路集团有限公司为了保证铁路项目施工质量,要求施工单位对铁路项目施工过程进行全方位监测。项目施工监测过程中的监测数据及施工影像需要统一存档至行业主管部门,保证施工质量可追溯,提高智慧施工的认知度,提升信息化管理水平。施工监测过程中的监测数据可以为工程结构优化设计、制定施工过程中的相关技术标准等提供数据支持。但在目前施工项目监测模式中,大量的数据分析、处理、存储操作给监测平台带来服务器负载高、网络带宽压力大、关键监测数据可能被篡改、安全事故责任难以确定等多方面的困难与挑战^[3]。按照国家铁路集团的要求,目前大多数铁路施工项目安装了信息化安全监测系统,但数据主管部门对安全监测数据的应用研究还处于数据展示、存储的初级阶段,对安全监测数据的共享研究较少。借鉴其他背景下的数据共享研究,不难发现监测数据共享存在着数据持有者共享意愿不强、数据共享利用不充分、数据潜在价值未激活等问题,这些问题同样遏制了铁路施工项目安全监测数据共享的发展^[4]。

在上述分析的基础上,本文提出了基于边缘计算的铁路施工项目安全监管数据可信共享模式,将边缘计算与铁路施工项目安全监测结合,

解决了服务器负载高和网络带宽压力大的问题。同时,为了解决监测数据共享过程中的数据安全性问题,将关键数据(如异常的应变、挠度信息等)存入区块链中,在保证数据安全的前提下,提高了数据共享性。

2 存在的问题

2.1 铁路施工项目在线监测

铁路施工项目监测主要是对项目结构体的结构、表面系数在荷载和自然环境下结构的响应(如应力、应变、挠度等),同时对结构的可靠性、耐久性,所处位置的温湿度等进行监测^[5]。铁路施工项目监测主要由硬件和软件两部分组成,硬件部分包括监测传感器设备、计算机、服务器等,软件部分包括数据采集与传输系统、数据分析与处理系统、数据库管理系统等。软硬件部分协作,完成铁路施工项目的安全监测。

目前的铁路施工项目安全监测模式主要以物联网监测模型为基础,结合云计算、BIM、传感技术等^[6]。铁路施工项目在线监测面临的问题主要表现在以下3个方面。

(1) 数据存储

安全监测数据通过无线或有线的通信方式传输至监测平台,而后依赖服务器算力进行数据处理、分析等工作,造成服务器负载大^[7],容易出现故障或宕机情况,同时数据量增加还会造成存储服务器成本增加。

(2) 数据传输

无线网络受网络带宽和速度的限制,导致大量监测数据传输时给网络带宽造成压力^[3],数据可能会出现传输时延大、传输过程丢失分组等现象。

(3) 数据安全

传统监测系统使用中心式存储方式,中心节点拥有系统全部权限,可能对监测数据执行伪造、删除等操作,无法保证数据的真实性^[7],可能造



成无法判断施工质量责任归属的情况发生。

2.2 安全监测数据共享

目前的数据共享研究应用主要集中于政务数据共享、医疗数据政务共享等，铁路施工项目安全监测数据的共享研究还未得到人们的重视，但安全监测数据是重要的施工过程记录之一，它可以直观地反映施工过程中的项目结构体的结构变化程度等重要信息。安全监测数据共享，可以供其他社会机构进行数据分析等工作，挖掘其潜在价值，因此安全监测数据共享不可或缺。但安全监测数据掌握在行业主管部门，安全监测数据难以实现共享。

目前数据可信共享模式面临的主要挑战如下。

(1) 对安全监测数据的共享意愿不强烈

在大数据时代，数据是第一生产力，各单位把数据视为自己部门的“私有财产”，不愿意共享开放，产生了数据互联互通的壁垒。

(2) 安全监测数据共享过程的安全性无法保证

数据共享很大程度上依赖于网络平台方式实现，若网络平台出现安全问题，导致安全监测数据被窃取或篡改，将会带来恶劣影响^[8]。

(3) 安全监测数据的共享设施建设不完善

在共享平台上存在数据接口不一、数据标准不一等问题，导致数据共享难。

3 铁路施工项目安全监管数据可信共享框架

3.1 层次结构

铁路施工项目安全监管数据可信共享模式设计以物联网架构为基础，在数据服务层利用区块链技术对数据存储方式进行改进，该模式架构如图1所示。施工项目安全监管数据可信共享模式根据功能属性分为4层，自下而上分别为感知层、边缘层、数据服务层、用户层。

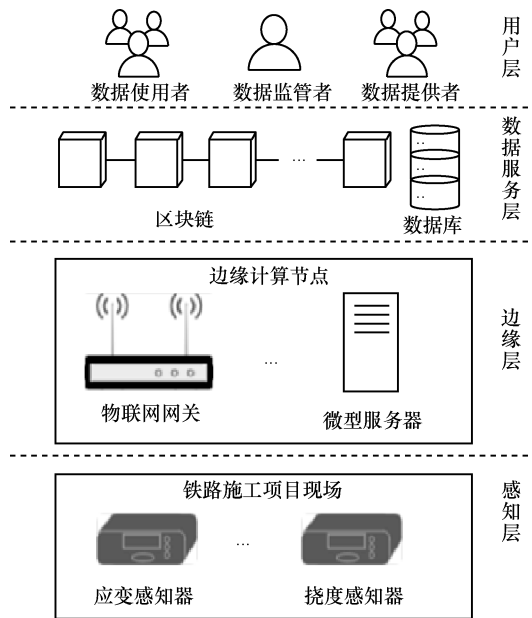


图1 铁路施工项目安全监管数据可信共享模式架构

感知层主要负责铁路施工项目结构体的结构信息（如应变、形变等）的获取，感知器通常包括表面式应变计、激光测距传感器等，可以为铁路项目施工过程中结构体的结构参数获取提供感知手段，为提高施工的安全性和施工管理水平提供物理设备支持，感知层设备与边缘层设备的通信方式主要采取有线方式。

边缘层主要为监测数据提供格式转换、缓存、处理、分析和传输服务，降低铁路施工项目安全监管数据可信共享模式中心服务器的负载，提高数据处理效率。边缘层设备包括物联网网关和微型服务器等，这些设备共同构成了边缘节点网络，为系统的边缘层提供了轻量级的计算能力，边缘层设备与数据服务层设备通过无线通信方式传输数据。

数据服务层是铁路施工项目安全监管数据可信共享模式的核心层，由区块链和数据库组成。由于区块链的吞吐能力较低，所以区块链网络用来存储监测过程中的数据量较少的异常数据；数据库用来存储监测过程中的正常数据。服务器执行监测数据的分类、二次处理、分析等计算任务，提供更复杂的数据处理和分析能力。

用户层是铁路施工项目安全监管数据可信共享模式与用户交互的客户端所在层,它为数据使用者、数据监管者、数据提供者提供数据共享数据监管等服务。数据共享是当数据使用者提出数据请求时,向其提供监测数据共享的服务窗口;数据监管是数据监管者对感知数据进行监督管理;此外,该层还提供其他如人员管理、设备管理等应用功能。

3.2 主要功能模块

铁路施工项目安全监管数据可信共享模式主要包含两个功能模块,分别为安全监测边缘计算模块和数据可信共享模块。

3.2.1 安全监测边缘计算模块

(1) 边缘计算

边缘计算指数据或任务能够在靠近数据源头的网络边缘侧进行计算和执行计算的一种新型服务模式^[9]。边缘计算设备包括物联网网关、轻量级服务器和小型基站等,这些设备能够提供轻量级的计算能力和数据处理能力,分担服务器的计算任务,减少上传至中心平台的数据量、额外传输能量消耗和降低服务器负载^[10]。边缘计算靠近终端提供轻量级计算和存储服务的特点,使其在各种场景监测中的应用越来越广泛,将边缘计算与铁路施工项目安全监测结合,可以缓解目前铁路施工项目安全监测中的服务器负载高和网络带宽压力大的问题。

(2) 铁路施工项目安全监测边缘计算框架

铁路施工项目安全监测边缘计算模块的设计框架如图2所示,边缘设备不仅可以将其共享客户端接收到的命令(如感知设备的增删改命令等)下发至感知设备,还可以执行部分计算任务,包括对接入的设备进行管理;支持用户层设备命令的下发、采集仪通道设定管理、感知设备的增加、删除与维护功能;监测数据经解析、转换处理后,调用异常数据处理函数对异常值进行判断,根据判断结果对监测数据进行处置;当出现网络中断

时,边缘设备可以对监测数据进行缓存。通过边缘计算设备,将部分属于共享平台服务器的数据处理步骤下放至边缘层,在边缘层实现设备管理、数据处理、数据缓存等功能,降低了网络带宽开支,减少了网络中断造成数据丢失的发生概率,提高了业务实时连续性,保证系统有效平稳运行。

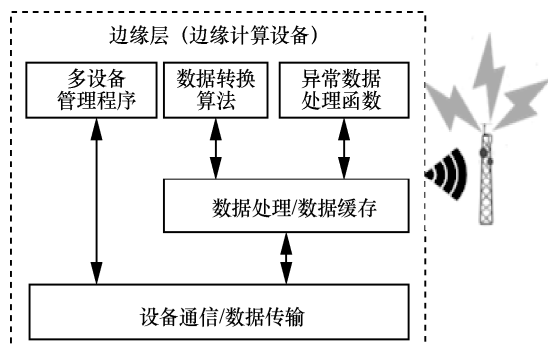


图2 铁路施工项目安全监测边缘计算模块的设计框架

3.2.2 数据可信共享模块

(1) 区块链

区块链是一种去中心化、难以篡改、可追溯、多方共同维护的分布式数据库,能够将传统单方维护的仅涉及自己业务的多个孤立数据库整合在一起,分布式地存储在多方共同维护的多个节点上,任何一方都无法完全控制这些数据,只能按照严格的规则和共识进行更新,从而实现了可信的、多方间的信息共享和监督,提高业务处理效率,降低交易成本^[11]。区块链使用共识机制、集成P2P协议、块链结构、智能合约、非对称加密等技术,解决数据的信任问题。通过区块链技术,可以在没有第三方机构的前提下,实现互不信任的多方对区块链内数据信息的可信与共享。区块链网络中各个节点都遵从特定的共识机制,具有难以篡改和高可信的特性,可以缓解现有的铁路施工项目安全监管数据可信共享中的数据安全性低、共享性差等问题。

(2) 铁路施工项目监测数据可信共享框架

基于联盟区块链的铁路施工项目可信数据共享模块的设计框架如图3所示。联盟链由若干个



经过授权的主体（形成联盟）共同参与管理，只允许系统内被授权的用户读写或提交交易^[11]。目前，应用最广泛的联盟链通用开发平台是 Hyperledger Fabric。在监测数据共享联盟区块链中，作为监管方的铁路施工项目监管部门对参与其中的各个铁路项目施工单位进行授权管理。

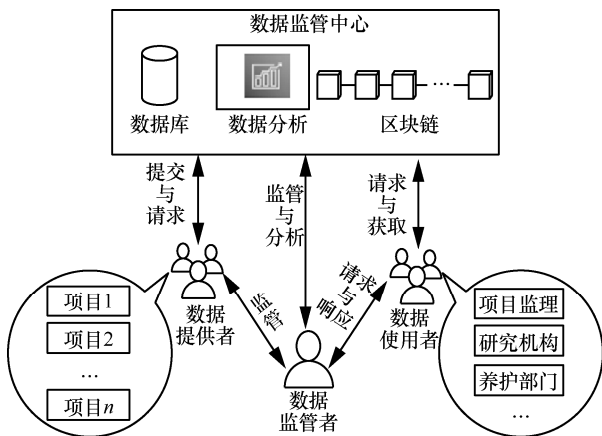


图3 铁路施工项目监测数据可信共享框架

数据共享模块内部主要由3种角色组成，分别是数据提供者、数据监管者、数据使用者。数据监管中心提供数据监管者的监测数据分析结果，使用区块链和数据库共同存储安全监测数据：数据库存储正常安全监测数据（在施工标准中结构体的结构物参数标准指标内），区块链存储在标准外的异常安全监测数据。采用这种存储方式可以解决：区块链的大量数据存储压力和高频率的访问压力问题；异常数据为敏感数据，相关责任人为了减轻安全事故责任可能会篡改或删除异常数据的问题。

数据提供者是感知器的安装者如施工现场的施工单位等利益相关方。数据提供者负责铁路项目的施工建造、铁路项目施工中的问题处置；根据数据监管者发送的命令对传感器和边缘计算设备进行安装、拆除、故障排查等。

数据监管者是铁路施工项目安全监管数据可信共享平台的运营维护单位和监测数据的监督管理单位。其履行铁路项目施工阶段的监管责任，查看是否按照设计单位的设计方案建设，确定现

有监测方案是否符合监测需求，在施工过程中发生事故时确定责任人等。还需要根据监测需求和监管政策，适时调整监测方案，并将修改命令发送给数据提供者。

数据使用者包括研究单位和铁路项目运营维护单位等施工阶段的其他非利益相关方，他们根据自身需求，请求共享安全监测数据。

3.3 监测数据共享区块链的智能合约设计

智能合约是区块链的核心构成要素，是由事件驱动的、具有状态的、运行在可复制的共享区块链数据账本上的计算机程序，能够主动或被动地处理数据，接受、存储和发送价值以及控制和管理各类链上智能资产等^[12]。铁路施工项目数据可信共享区块链的智能合约主要包括：身份控制合约（identity controller contract, ICC）、监测数据管理合约（monitoring data manage contract, MDMC）等，如图4所示。

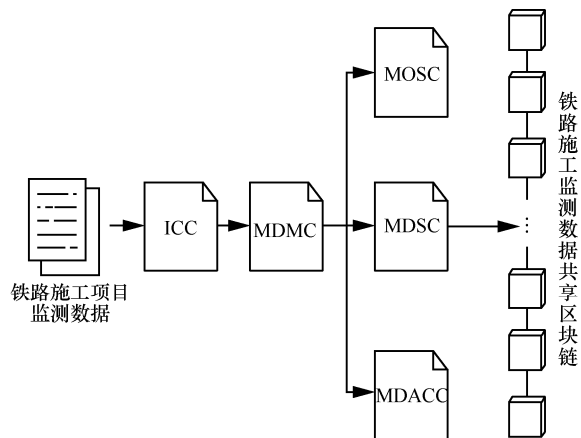


图4 智能合约体系

ICC 是记录区块链中所有用户（在本框架中一个项目代表一个用户）的数字身份标识（MO-ID）、对应的公钥（PubKey）、与其相关的MDMC的智能合约。在创建ICC时，第一个用户的数字身份以及相关合约被一同创建。

MDMC 用于实现保存在区块链中监测数据的存储、验证和共享等业务逻辑，包括监测对象存储合约（monitoring object storage contract,

MOSC)、监测信息共享合约 (monitoring data sharing contract, MDSC)、监测数据权限控制合约 (monitoring data authority control contract, MDACC)。MOSC 用于存储项目的主要信息, 包括项目的编号的哈希值、版本号、创建时间和最后的修改时间等; MDSC 用于存储施工项目的安全监测数据, 包括安全监测数据所属项目的编号、项目的数字身份标识和共享时间等。

(1) 新增监测对象

在新增监测对象 (monitoring object, MO) 时, 首先生成 MO 的数字身份标识 (MO-identify, 包括 MO 的名称、所在地、结构类型等属性的整合) 的哈希值 ($\text{Hash}_{\text{MO-I}}$) 和编号 MO-ID 等信息, 并对这些信息进行签名, 然后发送到智能合约进行处理。MOSC 接收到新增监测对象请求后, 调用 MDACC 从签名中回复公钥信息, 并与 ICC 中登记的密钥进行对比, 若验证通过, 则添加 MO-ID 等信息的映射, 其过程如算法 1 所示。

算法 1 新增监测对象

```

输入 监测对象 MO
输出 MO-ID 的映射
begin
  system executes
    MO-Identify ← combine(MO_name,
    MO_address, MO_structure)
    signature ← DSAsign(MO-ID, HashMO-I)
  contract executes
    if
      MDACC(signature, MO-ID)=true
    then
      MOSCmapping(MO-ID, [version,
      Hash, Time])
    end if
  end

```

(2) 数据共享

以共享者 (sharer) 请求共享监测对象 A

(MO-A) 的安全监测数据为例, sharer 首先对共享监测目标 A 的 MO-A-ID 进行签名, 然后将其发送到智能合约, MOSC 接收到请求后, 先调用 MDACC, 通过签名对 sharer 的身份进行核查, 核查通过后, 调用 MDSC 返回 MO-A-ID 的监测数据, 其过程如算法 2 所示。

算法 2 共享监测对象 A 的监测数据

```

输入 监测对象 MO-A
输出 MO-A 的监测数据
begin
  system executes
    sharer_signature ← DSAsharer(MO-A-ID)
  contract executes
    if
      MDACC(SHARER_signature)=true
    then
      Monitoring_data ← MDSC(MO-A-ID, [Monitoring_Data])
    end if
    return Monitoring_data
  end

```

4 工作流程

4.1 边缘计算节点中的监测数据处理流程

铁路施工项目现场边缘计算节点中的数据处理的包括多设备接入和管理、数据清洗与筛选。图 5 是铁路施工项目现场边缘节点监测数据处理流程。

(1) 多设备接入和管理

多设备接入和管理是边缘计算节点的基本功能, 是边缘网关和感知设备交互的第一步, 包含两部分内容: 设备连接与接入总线。每一部分都可以根据感知设备的类型进行独立开发。设备连接指的是边缘网关通过建立 TCP 连接和监听端口的方式与感知设备建立连接; 接入总线指利用消息总线实现设备注册和管理, 将感知设备的序列号、是否在线、所处节点等信息记录到设备管理表中。

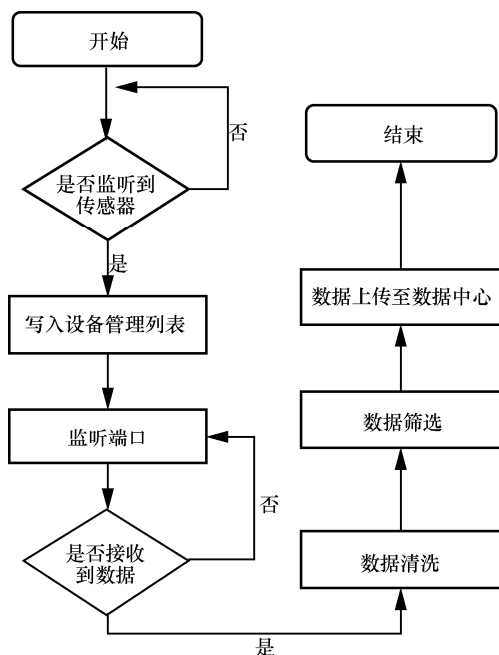


图5 监测数据处理流程

(2) 数据清洗与筛选

感知器将采集到的数据传输至边缘网关中，边缘网关需要对这些数据进行转换、筛选等，以达到提高数据质量、降低数据规模的目的。边缘设备最后将数据上传至系统平台，提高传输效率、降低传输成本。数据分析与清洗主要包含数据缺失值处理、数据转换和数据筛选。

(a) 缺失值处理

当某一条感知数据出现缺失时，需要对数据进行处理，使其不影响监测结果。因为含有缺失值的感知数据占比较低，所以可以直接丢弃含有缺失值的感知数据。

(b) 数据转换

指将感知设备传输的感知数据转换为同规范的数据格式。在监测系统中存在多种类型的感知器，通过这些感知器监测到的数据存在数据格式不统一、通信协议不统一的问题。监测数据进行传输时，需将这些数据转换成相同的数据格式后，再对数据作进一步处理等操作。以激光测距传感器 SW-LDS50A 为例，监测数据转换过程如算法 3 所示。

算法 3 激光测距传感器 SW-LDS50A 监测

数据转换算法

输入 十六进制八字节监测数据帧

输出 十进制字符型监测数据

...

switch(monitor){//选择传感器型号

...

case “SW-LDS50A”

monitor_data←HEX_monitor_data.Substring//截取监测数据帧中的监测数据部分
DEC_monitor_data← conversion (monitor_data)//将十六进制监测数据转为十进制监测数据

range←0.01*DEC_monitor_data//以激光测距传感器 SW-LDS50A 说明书所列公式求得距离值

break

...

}

...

(c) 数据筛选

感知数据经过缺失值处理和格式转换操作后，可根据其数据内容判断是否超过系统预设的该类数据限定值，若超过限定值，则将数据定性为异常数据，添加异常标识，方便系统平台对异常数据做进一步处理。减少系统服务器的负担，释放服务器算力，为数据分析提供便利条件。

4.2 铁路施工项目监测数据存储流程

(1) 监测数据正常

边缘计算设备实时与感知设备进行交互并对监测数据进行初步计算，若监测数据无异常，则向数据服务层发送正常监测数据，数据服务层将接收的数据存入对应的数据库中。边缘计算设备与数据服务层的服务器在规定时间内相互通信，确保服务器网络工作正常。

(2) 监测数据异常

边缘计算设备实时与感知设备进行交互并对

监测数据进行初步计算,若监测数据异常,则标记异常数据,向数据服务层发送异常监测数据,数据服务层将接收到的异常数据存入区块链中。

4.3 铁路施工项目监测数据共享流程

数据可信共享是指监测数据共享联盟链与外部用户之间通过智能合约和 PBFT 共识机制实现安全可靠的可信数据的共享,使得共享平台可以安全高效地从区块链系统获取可信数据,铁路施工项目数据可信共享流程如图 6 所示。

步骤 1 数据使用者通过数据共享平台向数据监管者发送自身的身份信息和数据共享请求 (sharing request, SR),包括请求共享的数据类型、时间节点、监测对象等信息。

步骤 2 数据监管者在数据共享平台查验数据使用者的身份信息是否满足数据共享要求,若查验符合要求则进入步骤 3;否则拒绝共享请求。

步骤 3 数据共享平台向数据中心发送数据请

求方的 SR。

步骤 4 数据中心查验 SR 内的信息。

步骤 5 数据中心根据 SR 内的信息,判断数据所在地,请求异常数据则向区块链发送请求信息,请求正常数据则向数据库发送请求信息。

步骤 6 区块链和数据库响应请求信息,将所需数据发送给数据共享平台。

步骤 7 数据共享平台向数据请求方返回共享数据。

5 结束语

目前,基于本文提出的铁路施工项目安全监管方案,开发了在建桥梁主体结构监测云平台,实际应用中已采集京雄高铁在建桥梁监测数据数百万条,实现了多个施工项目安全监测数据的实时采集、分析、预警等功能,该平台拟接入铁路在建项目监测数据中心,拓展其应用范围。在后

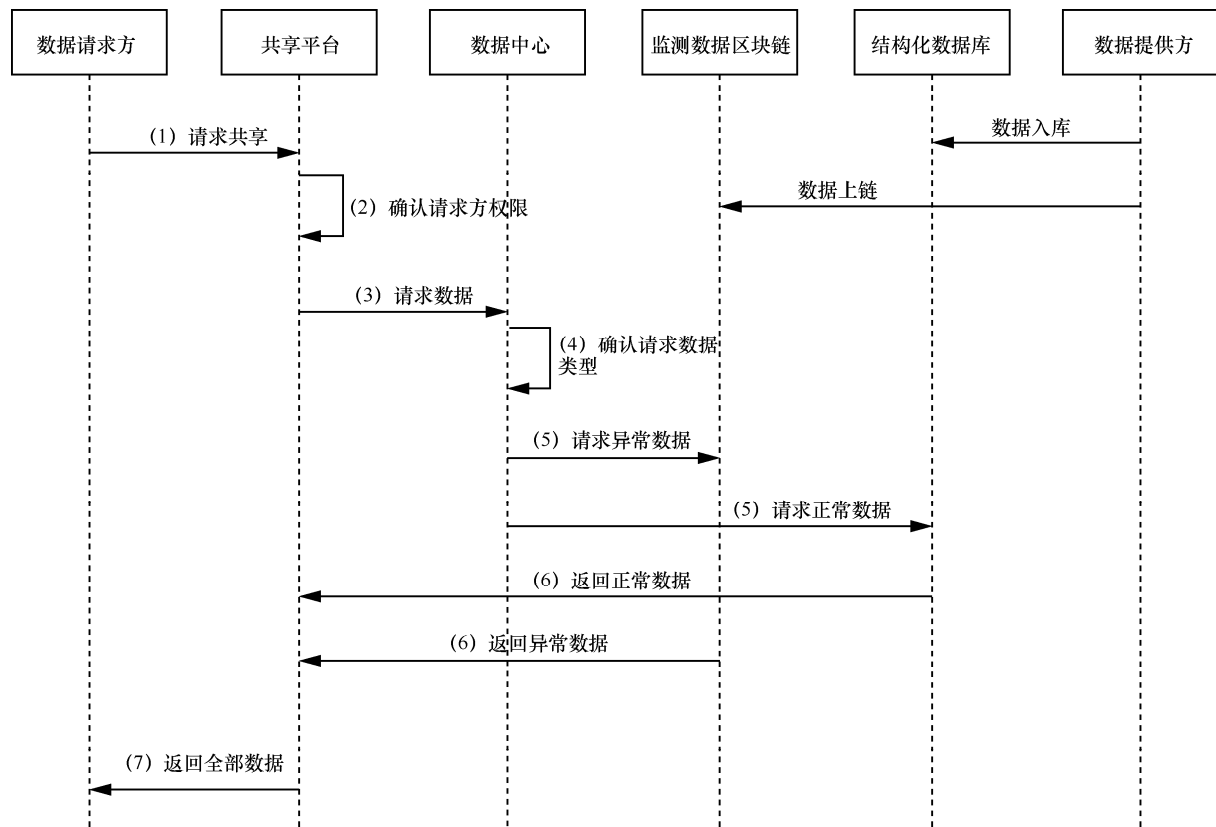


图 6 铁路施工项目数据可信共享流程



续的研发工作中，将利用大数据技术，对安全监测数据潜在价值进行深度挖掘分析，并结合区块链技术实现铁路工程施工项目安全监管数据多方可信共享。

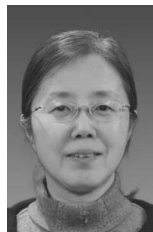
参考文献：

- [1] 邱铁鑫. 新时代“交通强国”战略的理论探析[J]. 北京交通大学学报(社会科学版), 2019, 18(4): 58-62, 92.
QIU T X. Theoretical inquiry into the strategy of “Building China’s strength in transportation” in the new era[J]. Journal of Beijing Jiaotong University (Social Sciences Edition), 2019, 18(4): 58-62, 92.
- [2] 唐建平. 微结构光纤分布式传感系统在铁路安全监测中的应用研究[J]. 建筑施工, 2020, 42(2): 270-272.
TANG J P. Research on application of micro structural optical fiber distributed sensing system in railway safety monitoring[J]. Building Construction, 2020, 42(2): 270-272.
- [3] 赵梓铭, 刘芳, 蔡志平, 等. 边缘计算: 平台、应用与挑战[J]. 计算机研究与发展, 2018, 55(2): 327-337.
ZHAO Z M, LIU F, CAI Z P, et al. Edge computing: platforms, applications and challenges[J]. Journal of Computer Research and Development, 2018, 55(2): 327-337.
- [4] 郭明军, 童楠楠, 王建冬. 政务数据与社会数据共享利用中存在的问题及应对举措[J]. 中国经贸导刊, 2019(8): 37-38.
GUO M J, TONG N N, WANG J D. Problems and countermeasures in the sharing and utilization of government data and social data[J]. China Economic & Trade Herald, 2019(8): 37-38.
- [5] 吴学林. 桥梁健康监测系统集成及发展[J]. 南方农机, 2018, 49(14): 112.
WU X L. Construction and development of bridge health monitoring system[J]. China Southern Agricultural Machinery, 2018, 49(14): 112.
- [6] 刘占省, 孙佳佳, 杜修力, 等. 智慧建造内涵与发展趋势及关键应用研究[J]. 施工技术, 2019, 48(24): 1-7, 15.
LIU Z S, SUN J J, DU X L, et al. Smart construction connotation and development trend and key application research[J]. Construction Technology, 2019, 48(24): 1-7, 15.
- [7] 柏亮. 区块链技术在工业物联网的应用研究[J]. 网络空间安全, 2018, 9(9): 87-91.
BAI L. Application and research of blockchain technology in industrial internet of things[J]. Cyberspace Security, 2018, 9(9): 87-91.
- [8] 马海群, 江尚谦. 我国政府数据开放的共享机制研究[J]. 图书情报研究, 2018, 11(1): 3-11.
MA H Q, JIANG S Q. The sharing mechanism of China’s open government data[J]. Library and Information Studies, 2018, 11(1): 3-11.
- [9] 张佳乐, 赵彦超, 陈兵, 等. 边缘计算数据安全性与隐私保护研究综述[J]. 通信学报, 2018, 39(3): 1-21.
ZHANG J L, ZHAO Y C, CHEN B, et al. Survey on data security and privacy-preserving for the research of edge computing[J]. Journal on Communications, 2018, 39(3): 1-21.
- [10] 李邱苹, 赵军辉, 贡毅. 移动边缘计算中的计算卸载和资源管理方案[J]. 电信科学, 2019, 35(3): 36-46.
LI Q P, ZHAO J H, GONG Y. Computation offloading and resource management scheme in mobile edge computing[J]. Telecommunications Science, 2019, 35(3): 36-46.
- [11] 邵奇峰, 金澈清, 张召, 等. 区块链技术: 架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.
- [12] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.
YUAN Y, WANG F Y. Blockchain: the state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[作者简介]



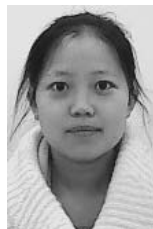
杨亮 (1994—)，男，石家庄铁道大学信息科学与技术学院硕士生，主要从事大数据、区块链技术及其应用研究工作。



朴春慧 (1964—)，女，石家庄铁道大学信息科学与技术学院教授、硕士生导师，主要从事信息管理与信息系统、数据安全与隐私保护等方面的研究工作。



刘玉红 (1974—)，男，石家庄铁道大学信息科学与技术学院副教授，中国铁路集团信息化委员会委员，主要从事结构安全监测、施工监测等方面的研究工作。



冀梅梅 (1996—)，女，石家庄铁道大学信息科学与技术学院硕士生，主要从事大数据技术及其应用研究工作。